ACG1000是否涉及OpenSSH ProxyCommand命令注入漏洞（CVE-2023-51385）

漏洞扫描 卢鹏 2024-05-28 发表

漏洞相关信息

漏洞编号： CVE-2023-51385
漏洞名称： OpenSSH ProxyCommand命令注入漏洞
产品型号及版本： ACG1000

漏洞描述

一、漏洞背景

OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。SSH协议族可以用来进行远程控制， 或在计算机之间传送文件。而实现此功能的传统方式，如telnet(终端仿真协议)、 rcp ftp、 rlogin、rsh都是极为不安全的，并且会使用明文传送密码。OpenSSH提供了服务端后台程序和客户端工具，用来加密远程控制和文件传输过程中的数据，并由此来代替原来的类似服务。近日，新华三盾山实验室监测到OpenSSH官方发布了安全公告，修复了一个存在于OpenSSH中的命令注入漏洞（CVE-2023-51385），攻击者可利用该漏洞注入恶意Shell字符导致命令注入。

二、漏洞详情

此漏洞是由于OpenSSH中的ProxyCommand命令未对%h、%p或类似的扩展标记进行正确的过滤，攻击者可通过这些值注入恶意shell字符进行命令注入攻击。

三、影响范围

OpenSSH<9.6

漏洞解决方案

不涉及